QUIZ 7

Security

Question 1

A replaying attack is best defined as:

- a) Falsely receiving the same message multiple times.
- b) Sending or receiving messages using the identify of another principal.
- c) Intercepting messages and altering their contents before passing them on.
- **d) Storing intercepted messages and sending them at a later date.**
- e) Intercepting messages and sending them back to the sender as if they came from the receiver.

Question 2

Considering a public/private key pair, which of the following is not true?

- **a) The public key can be used to create digital signature.**
- b) The private key can be used to create a digital signature.
- c) Documents encrypted with the public key can only be decrypted with the private key.
- d) Documents encrypted with the private key can only be decrypted with the public key.
- e) The private key must be securely stored.

Question 3

Symmetric encryption is used for session encryption, rather than asymmetric encryption because:

- a) It is much stronger than asymmetric encryption.
- b) It does not require as much memory as asymmetric encryption.
- c) More protocols are available for asymmetric encryption.
- **d) It is much faster than asymmetric encryption.**
- e) None of the above reasons.

Question 4

Which one of the following encryption algorithms is not a symmetric algorithm?

- a) TEA
- b) DES
- **c) RSA**
- d) IDEA
- e) AES

Question 5

Which of the following is not a property of a secure digest function h = H(M)?

- a) Given M, it is easy to compute h.
- **b) Given h, it is easy to compute M.**
- c) Given h, it is hard to compute M.
- d) Given M, it is hard to find another message M', such that H(M) = H(M').
- e) It is possible for two messages M and M' to have the same hash values. That is, it is possible that H(M) = H(M') for some M and M'.

Question 6

What is inside a Kerberos ticket?

- **a) The session key.**
- b) A challenge message.
- c) The client's digital certificate.
- d) A handle to a Kerberos authentication structure within the Kerberos authentication server.
- e) The client's public key.

Question 7

In symmetric cryptography, which of the following must be true:

- a) Encryption and decryption take the same amount of time.
- b) Different algorithms are used for encryption and decryption.
- c) Cryptographic operations are one-way, and not reversible.
- **d) The same key is used for encryption and decryption.**
- e) Both c) and d).

Question 8

Which of the following can I do without knowing your private key?

- a) Pretend to send a private message on your behalf
- b) Decrypt messages that were intended for only you
- **c) Send you a message that only you can read**
- d) Digitally sign a message on your behalf
- e) I must know your private key to perform all of these operations

Question 9

Which of the following issues is not addressed by Kerberos:

- **a) Availability.**
- b) Privacy.
- c) Integrity.
- d) Authentication.
- e) All of the above issues are addressed by Kerberos.

Question 10

SHA and MD5 are examples of:

- a) Symmetric block ciphers.
- b) Asymmetric block ciphers.
- c) Symmetric stream ciphers.
- d) Asymmetric stream ciphers.
- **e) Secure digest functions.**